PCT

REQUÊTE

Le soussigné requiert que la présente demande internationale soit traitée conformément au Traité de coopération en matière de brevets:

Réservé à l'office récepteur

Demande internationale n°

Date du dépôt international

Nom de l'office récepteur et "Demande internationale PCT"

Référence du dossier du déposant ou du mandataire *(facultatif)* *(12 caractères au maximum)* PCT 3857/BC

Cadre n° I TITRE DE L'INVENTION

PROCEDE DE SECURISATION D'UN ENSEMBLE ELECTRONIQUE DE CRYPTOGRAPHIE A BASE D'EXPONENTIATION MODULAIRE CONTRE LES ATTAQUES PAR ANALYSE PHYSIQUE.

Cadre n° II DÉPOSANT

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

BULL CP8
68, route de Versailles
BP 45
78430 LOUVECIENNES
FRANCE

☐ Cette personne est aussi inventeur.

n° de téléphone (33) 1 39.66.61.76

n° de télécopieur (33) 1 39.66.61.73

n° de téléimprimeur

Nationalité (nom de l'État) : FRANCE

Domicile (nom de l'État) : FRANCE

Cette personne est déposant pour : ☐ tous les États désignés ☒ tous les États désignés sauf les États-Unis d'Amérique ☐ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

Cadre n° III AUTRE(S) DÉPOSANT(S) OU (AUTRE(S)) INVENTEUR(S)

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

GOUBIN Louis
3 rue Brown Séquard
75015 PARIS
FRANCE

Cette personne est :

☐ déposant seulement

☒ déposant et inventeur

☐ inventeur seulement *(Si cette case est cochée, ne pas remplir la suite.)*

Nationalité (nom de l'État) : FRANCE

Domicile (nom de l'État) : FRANCE

Cette personne est déposant pour : ☐ tous les États désignés ☐ tous les États désignés sauf les États-Unis d'Amérique ☒ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

☐ D'autres déposants ou inventeurs sont indiqués sur une feuille annexe.

Cadre n° IV MANDATAIRE OU REPRÉSENTANT COMMUN; OU ADRESSE POUR LA CORRESPONDANCE

La personne dont l'identité est donnée ci-dessous est/a été désignée pour agir au nom du ou des déposants auprès des autorités internationales compétentes, comme: ☒ mandataire ☐ représentant commun

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays.)*

BULL S.A
CORLU Bernard
PC58D20 / 68, route de Versailles
F- 78434 LOUVECIENNES Cedex (FRANCE)

n° de téléphone (33) 1 39.66.61.76

n° de télécopieur (33) 1 39.66.61.73

n° de téléimprimeur

☐ **Adresse pour la correspondance :** cocher cette case lorsque aucun mandataire ni représentant commun n'est/n'a été désigné et que l'espace ci-dessus est utilisé pour indiquer une adresse spéciale à laquelle la correspondance doit être envoyée.

PCT 754/301299

Cadre n° V DÉSIGNATION D'ÉTATS

Les désignations suivantes sont faites conformément à la règle 4.9.a) *(cocher les cases appropriées; une au moins doit l'être)* :

Brevet régional

☐ **AP** **Brevet ARIPO** : **GH** Ghana, **GM** Gambie, **KE** Kenya, **LS** Lesotho, **MW** Malawi, **SD** Soudan, **SL** Sierra Leone, **SZ** Swaziland, **TZ** République-Unie de Tanzanie, **UG** Ouganda, **ZW** Zimbabwe et tout autre État qui est un État contractant du Protocole de Harare et du PCT

☐ **EA** **Brevet eurasien** : **AM** Arménie, **AZ** Azerbaïdjan, **BY** Bélarus, **KG** Kirghizistan, **KZ** Kazakhstan, **MD** République de Moldova, **RU** Fédération de Russie, **TJ** Tadjikistan, **TM** Turkménistan et tout autre État qui est un État contractant de la Convention sur le brevet eurasien et du PCT

☒ **EP** **Brevet européen** : **AT** Autriche, **BE** Belgique, **CH et LI** Suisse et Liechtenstein, **CY** Chypre, **DE** Allemagne, **DK** Danemark, **ES** Espagne, **FI** Finlande, **FR** France, **GB** Royaume-Uni, **GR** Grèce, **IE** Irlande, **IT** Italie, **LU** Luxembourg, **MC** Monaco, **NL** Pays-Bas, **PT** Portugal, **SE** Suède et tout autre État qui est un État contractant de la Convention sur le brevet européen et du PCT

☐ **OA** **Brevet OAPI** : **BF** Burkina Faso, **BJ** Bénin, **CF** République centrafricaine, **CG** Congo, **CI** Côte d'Ivoire, **CM** Cameroun, **GA** Gabon, **GN** Guinée, **GW** Guinée-Bissau, **ML** Mali, **MR** Mauritanie, **NE** Niger, **SN** Sénégal, **TD** Tchad, **TG** Togo et tout autre État qui est un État membre de l'OAPI et un État contractant du PCT *(si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée)* .....

Brevet national *(si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée)* :

☐ **AE** Émirats arabes unis
☐ **AL** Albanie .....
☐ **AM** Arménie .....
☐ **AT** Autriche .....
☐ **AU** Australie .....
☐ **AZ** Azerbaïdjan
☐ **BA** Bosnie-Herzégovine .....
☐ **BB** Barbade
☐ **BG** Bulgarie .....
☐ **BR** Brésil .....
☐ **BY** Bélarus .....
☐ **CA** Canada
☐ **CH et LI** Suisse et Liechtenstein
☐ **CN** Chine .....
☐ **CR** Costa Rica .....
☐ **CU** Cuba .....
☐ **CZ** République tchèque .....
☐ **DE** Allemagne .....
☐ **DK** Danemark .....
☐ **DM** Dominique
☐ **EE** Estonie .....
☐ **ES** Espagne .....
☐ **FI** Finlande .....
☐ **GB** Royaume-Uni
☐ **GD** Grenade
☐ **GE** Géorgie .....
☐ **GH** Ghana .....
☐ **GM** Gambie
☐ **HR** Croatie .....
☐ **HU** Hongrie .....
☐ **ID** Indonésie
☐ **IL** Israël .....
☐ **IN** Inde .....
☐ **IS** Islande
☒ **JP** Japon .....
☐ **KE** Kenya .....
☐ **KG** Kirghizistan .....
☐ **KP** République populaire démocratique de Corée .....
☐ **KR** République de Corée .....
☐ **KZ** Kazakhstan .....
☐ **LC** Sainte-Lucie
☐ **LK** Sri Lanka
☐ **LR** Liberia
☐ **LS** Lesotho .....
☐ **LT** Lituanie
☐ **LU** Luxembourg
☐ **LV** Lettonie
☐ **MA** Maroc .....
☐ **MD** République de Moldova .....
☐ **MG** Madagascar .....
☐ **MK** Ex-République yougoslave de Macédoine .....
☐ **MN** Mongolie
☐ **MW** Malawi .....
☐ **MX** Mexique .....
☐ **NO** Norvège
☐ **NZ** Nouvelle-Zélande .....
☐ **PL** Pologne .....
☐ **PT** Portugal .....
☐ **RO** Roumanie
☐ **RU** Fédération de Russie .....
☐ **SD** Soudan
☐ **SE** Suède
☐ **SG** Singapour
☐ **SI** Slovénie .....
☐ **SK** Slovaquie .....
☐ **SL** Sierra Leone .....
☐ **TJ** Tadjikistan .....
☐ **TM** Turkménistan .....
☐ **TR** Turquie .....
☐ **TT** Trinité-et-Tobago .....
☐ **TZ** République-Unie de Tanzanie
☐ **UA** Ukraine .....
☐ **UG** Ouganda .....
☒ **US** États-Unis d'Amérique .....
☐ **UZ** Ouzbékistan .....
☐ **VN** Viet Nam .....
☐ **YU** Yougoslavie .....
☐ **ZA** Afrique du Sud .....
☐ **ZW** Zimbabwe .....

Cases réservées pour la désignation d'États qui sont devenus parties au PCT après la publication de la présente feuille :

☐ .....
☐ .....

Déclaration concernant les désignations de précaution : outre les désignations faites ci-dessus, le déposant fait aussi conformément à la règle 4.9.b) toutes les désignations qui seraient autorisées en vertu du PCT, à l'exception de toute désignation indiquée dans le cadre supplémentaire comme étant exclue de la portée de cette déclaration. Le déposant déclare que ces désignations additionnelles sont faites sous réserve de confirmation et que toute désignation qui n'est pas confirmée avant l'expiration d'un délai de 15 mois à compter de la date de priorité doit être considérée comme retirée par le déposant à l'expiration de ce délai. *(La confirmation (y compris les taxes) doit parvenir à l'office récepteur dans le délai de 15 mois.)*

Voir les notes relatives au formulaire de requête

Cadre n° VI REVENDICATION DE PRIORITÉ ☐ D'autres revendications de priorité sont indiquées dans le cadre supplémentaire.

Date de dépôt de la demande antérieure *(jour/mois/année)*	Numéro de la demande antérieure	Lorsque la demande antérieure est une : demande nationale : pays	demande régionale :* office régional	demande internationale : office récepteur
(1) 28 octobre 1999 (28.10.1999)	99 13507	FRANCE		
(2)				
(3)				

☒ L'office récepteur est prié de préparer et de transmettre au Bureau international une copie certifiée conforme de la ou des demandes antérieures *(seulement si la demande antérieure a été déposée auprès de l'office qui, aux fins de la présente demande internationale, est l'office récepteur)* indiquées ci-dessus au(x) point(s) : 1

** Si la demande antérieure est une demande ARIPO, il est obligatoire d'indiquer dans le cadre supplémentaire au moins un pays partie à la Convention de Paris pour la protection de la propriété industrielle pour lequel cette demande antérieure a été déposée (règle 4.10.b)ii)). Voir le cadre supplémentaire.*

Cadre n° VII ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

Choix de l'administration chargée de la recherche internationale (ISA) *(si plusieurs administrations chargées de la recherche internationale sont compétentes pour procéder à la recherche internationale, indiquer l'administration choisie; le code à deux lettres peut être utilisé) :*
ISA/

Demande d'utilisation des résultats d'une recherche antérieure; mention de cette recherche *(si une recherche antérieure a été effectuée par l'administration chargée de la recherche internationale ou demandée à cette dernière) :*

Date *(jour/mois/année)*	Numéro	Pays *(ou office régional)*
28.10.99	99 13507 FA 583151	FR

Cadre n° VIII BORDEREAU; LANGUE DE DÉPÔT

La présente demande internationale contient le **nombre de feuilles** suivant :

requête	03
description (sauf partie réservée au listage des séquences)	10
revendications	02
abrégé	01
dessins	01
partie de la description réservée au listage des séquences	
Nombre total de feuilles	17

Le ou les éléments cochés ci-après **sont joints** à la présente demande internationale :

1. ☐ feuille de calcul des taxes
2. ☐ pouvoir distinct signé
3. ☒ copie du pouvoir général; numéro de référence, le cas échéant : 2
4. ☐ explication de l'absence d'une signature
5. ☒ document(s) de priorité indiqué(s) dans le cadre n° VI au(x) point(s) : 1
6. ☐ traduction de la demande internationale en (langue) :
7. ☐ indications séparées concernant des micro-organismes ou autre matériel biologique déposés
8. ☐ listage des séquences de nucléotides ou d'acides aminés sous forme déchiffrable par ordinateur
9. ☒ autres éléments *(préciser)* : Rapport de Recherche FA 583151

Figure des dessins qui doit accompagner l'abrégé :

Langue de dépôt de la demande internationale : FRANCAIS

Cadre n° IX SIGNATURE DU DÉPOSANT OU DU MANDATAIRE

À côté de chaque signature, indiquer le nom du signataire et, si cela n'apparaît pas clairement à la lecture de la requête, à quel titre l'intéressé signe.

CORLU Bernard (mandataire)

Réservé à l'office récepteur

1. Date effective de réception des pièces supposées constituer la demande internationale :
2. Dessins : ☐ reçus : ☐ non reçus :
3. Date effective de réception, rectifiée en raison de la réception ultérieure, mais dans les délais, de documents ou de dessins complétant ce qui est supposé constituer la demande internationale :
4. Date de réception, dans les délais, des corrections demandées selon l'article 11.2) du PCT :
5. Administration chargée de la recherche internationale (si plusieurs sont compétentes) : ISA/
6. ☐ Transmission de la copie de recherche différée jusqu'au paiement de la taxe de recherche.

Réservé au Bureau international

Date de réception de l'exemplaire original par le Bureau international :

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

Direction de la Propriété Intellectuelle

PCT

NOTIFICATION DE LA RECEPTION DE L'EXEMPLAIRE ORIGINAL

(règle 24.2.a) du PCT)

Destinataire:

12 DEC. 2000

BULL S.A.
Corlu, Bernard
PC58D20
68, route de Versailles
F-78434 Louveciennes cedex
FRANCE

BULL S.A.

Date d'expédition (jour/mois/année)	**NOTIFICATION IMPORTANTE**
22 novembre 2000 (22.11.00)	
Référence du dossier du déposant ou du mandataire	**Demande internationale no**
PCT 3857/BC	PCT/FR00/02978

Il est notifié au déposant que le Bureau international a reçu l'exemplaire original de la demande internationale précisée ci-après.

Nom(s) du ou des déposants et de l'Etat ou des Etats pour lesquels ils sont déposants:

BULL CP8 (pour tous les Etats désignés sauf US)
GOUBIN, Louis (pour US seulement)

Date du dépôt international	:	26 octobre 2000 (26.10.00)
Date(s) de priorité revendiquée(s)	:	28 octobre 1999 (28.10.99)
Date de réception de l'exemplaire original par le Bureau international	:	16 novembre 2000 (16.11.00)
Liste des offices désignés	:	

EP :AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE
National :JP,US

ATTENTION

Le déposant doit soigneusement vérifier les indications figurant dans la présente notification. En cas de divergence entre ces indications et celles que contient la demande internationale, il doit aviser immédiatement le Bureau international.

En outre, l'attention du déposant est appelée sur les renseignements donnés dans l'annexe en ce qui concerne

- [X] les délais dans lesquels doit être abordée la phase nationale
- [X] la confirmation des désignations faites par mesure de précaution
- [X] les exigences relatives aux documents de priorité.

Une copie de la présente notification est envoyée à l'office récepteur et à l'administration chargée de la recherche internationale.

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

n° de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé

Jocelyne Rey-Millet

n° de téléphone (41-22) 338.83.38

ANNEXE DU FORMULAIRE PCT/IB/301

de internationale no
PCT/FR00/02978

RENSEIGNEMENTS CONCERNANT LES DELAIS DANS LESQUELS DOIT ETRE ABORDEE LA PHASE NATIONALE

Il est rappelé au déposant qu'il doit aborder la "phase nationale" auprès de chacun des offices désignés indiqués sur la notification de la réception de l'exemplaire original (formulaire PCT/IB/301) en payant les taxes nationales et en remettant les traductions, telles qu'elles sont prescrites par les législations nationales.

Le délai d'accomplissement de ces actes de procédure est de **20 MOIS** à compter dela date de priorité ou, pour les Etats désignés qui ont été élus par le déposant dans une demande d'examen préliminaire international ou dans une élection ultérieure, de **30 MOIS** à compter de la date de priorité, à condition que cette électionait été effectuée avant l'expiration du 19e mois à compter de la date de priorité. Certains offices désignés (ou élus) ont fixé des délais qui expirent au-delà de 20 ou 30 mois à compter de la date de priorité. D'autres offices accordent une prolongation des délais ou un délai de grâce, dans certains cas moyennant le paiement d'une taxe supplémentaire.

En plus de ces actes de procédure, le déposant devra dans certains cas satisfaire à d'autres exigences particulières applicables dans certains offices. **Il appartient au déposant** de veiller à remplir en temps voulu les conditions requises pour l'ouverture de la phase nationale. La majorité des offices désignés n'envoient pas de rappel à l'approche de la date limite pour aborder la phase nationale.

Des informations détaillées concernant les actes de procédure à accomplir pour aborder la phase nationale auprès de chaque office désigné, les délais applicables et la possibilité d'obtenir une prolongation des délais ou un délai de grâce et toutes autres conditions applicables figurent dans le volume II du Guide du déposant du PCT. Les exigences concernant le dépôt d'une demande d'examen préliminaire international sont exposées dans le chapitre IX du volume I du Guide du déposant du PCT.

GR et ES sont devenues liées par le chapitre II du PCT le 7 septembre 1996 et le 6 septembre1997, respectivement, et peuvent donc être élues dans une demande d'examen préliminaire international ou dans une élection ultérieure présentée le 7 septembre 1996 (ou à une date postérieure) ou le 6 septembre 1997 (ou à une date postérieure), respectivement, quelle que soit la date de dépôt de la demande internationale (voir le second paragraphe, ci-dessus).

Veuillez noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

CONFIRMATION DES DESIGNATIONS FAITES PAR MESURE DE PRECAUTION

Seules les désignations expresses faites dans la requête conformément à la règle 4.9.a) figurent dans la présente notification. Il est important de vérifier si ces désignations ont été faites correctement. Des erreurs dans les désignations peuvent être corrigées lorsque des désignations ont été faites par mesure de précaution en vertu de la règle 4.9.b). Toute désignation ainsi faite peut être confirmée conformément aux dispositions de la règle 4.9.c) avant l'expiration d'un délai de 15 mois à compter de la date de priorité. En l'absence de confirmation, une désignation faite par mesure de précaution sera considérée comme retirée par le déposant. Il ne sera adressé aucun rappel ni invitation. Pour confirmer une désignation , il faut déposer une déclaration précisant l'Etat désigné concerné (avec l'indication de la forme de protection ou de traitement souhaitée) et payer les taxes de désignation et de confirmation. La confirmation doit parvenir à l'office récepteur dans le délai de 15 mois.

EXIGENCES RELATIVES AUX DOCUMENTS DE PRIORITE

Pour les déposants qui n'ont pas encore satisfait aux exigences relatives aux documents de priorité, il est rappelé ce qui suit.

Lorsque la priorité d'une demande nationale, régionale ou internationale antérieure est revendiquée, le déposant doit présenter une copie de cette demande antérieure, certifiée conforme par l'administration auprès de laquelle elle a été déposée ("document de priorité"), à l'office récepteur (qui la transmettra au Bureau international) ou directement au Bureau international, avant l'expiration d'un délai de 16 mois à compter de la date de priorité, étant entendu que tout document de priorité peut être présenté au Bureau international avant la date de publication de la demande internationale, auquel cas ce document sera réputé avoir été reçu par le Bureau international le dernier jour du délai de 16 mois (règle 17.1.a)).

Lorsque le document de priorité est délivré par l'office récepteur, le déposant peut, au lieu de présenter ce document, demander à l'office récepteur de le préparer et de le transmettre au Bureau international. La requête à cet effet doit être formulée avant l'expiration du délai de 16 mois et peut être soumise au paiement d'une taxe (règle 17.1.b)).

Si le document de priorité en question n'est pas fourni au Bureau international, ou si la demande adressée à l'office récepteur de préparer et de transmettre le document de priorité n'a pas été faite (et la taxe correspondante acquittée, le cas échéant) avant l'expiration du délai applicable mentionné aux paragraphes précédents, tout Etat désigné peut ne pas tenir compte de la revendication de priorité; toutefois, aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Lorsque plusieurs priorités sont revendiquées, la date de priorité à prendre en considération aux fins du calcul du délai de 16 mois est la date du dépôt de la demande la plus ancienne dont la priorité est revendiquée.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

AVIS INFORMANT LE DEPOSANT DE LA COMMUNICATION DE LA DEMANDE INTERNATIONALE AUX OFFICES DESIGNES

(règle 47.1.c), première phrase, du PCT)

Destinataire:
BULL S.A.
Corlu, Bernard
PC58D20
68, route de Versailles
F-78434 Louveciennes cedex
FRANCE

Date d'expédition (jour/mois/année)	
03 mai 2001 (03.05.01)	
Référence du dossier du déposant ou du mandataire PCT 3857/BC	**AVIS IMPORTANT**

Demande internationale no	**Date du dépôt international** (jour/mois/année)	**Date de priorité** (jour/mois/année)
PCT/FR00/02978	26 octobre 2000 (26.10.00)	28 octobre 1999 (28.10.99)

Déposant
BULL CP8 etc

1. Il est notifié par la présente qu'à la date indiquée ci-dessus comme date d'expédition de cet avis, le Bureau international a communiqué, comme le prévoit l'article 20, la demande internationale aux offices désignés suivants:
   US

   Conformément à la règle 47.1.c), troisième phrase, ces offices acceptent le présent avis comme preuve déterminante du fait que la communication de la demande internationale a bien eu lieu à la date d'expédition indiquée plus haut, et le déposant n'est pas tenu de remettre de copie de la demande internationale à l'office ou aux offices désignés.

2. Les offices désignés suivants ont renoncé à l'exigence selon laquelle cette communication doit être effectuée à cette date:
   EP,JP

   La communication sera effectuée seulement sur demande de ces offices. De plus, le déposant n'est pas tenu de remettre de copie de la demande internationale aux offices en question (règle 49.1)a-bis)).

3. Le présent avis est accompagné d'une copie de la demande internationale publiée par le Bureau international le
   03 mai 2001 (03.05.01) sous le numéro WO 01/31436

RAPPEL CONCERNANT LE CHAPITRE II (article 31.2)a) et règle 54.2)

Si le déposant souhaite reporter l'ouverture de la phase nationale jusqu'à 30 mois (ou plus pour ce qui concerne certains offices) à compter de la date de priorité, **la demande d'examen préliminaire international** doit être présentée à l'administration compétente chargée de l'examen préliminaire international avant l'expiration d'un délai de 19 mois à compter de la date de priorité.

Il appartient exclusivement au déposant de veiller au respect du délai de 19 mois.

Il est à noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

RAPPEL CONCERNANT L'OUVERTURE DE LA PHASE NATIONALE (article 22 ou 39.1))

Si le déposant souhaite que la demande internationale procède en phase nationale, il doit, dans le délai de 20 mois ou de 30 mois, ou plus pour ce qui concerne certains offices, accomplir les actes mentionnés dans ces dispositions auprès de chaque office désigné ou élu.

Pour d'autres informations importantes concernant les délais et les actes à accomplir pour l'ouverture de la phase nationale, voir l'annexe du formulaire PCT/IB/301 (Notification de la réception de l'exemplaire original) et le volume II du Guide du déposant du PCT.

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé
J. Zahra

no de téléphone (41-22) 338.83.38

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
PCT 3857/BC		
Demande internationale n°	Date du dépôt international *(jour/mois/année)*	(Date de priorité (la plus ancienne) *(jour/mois/année)*
PCT/FR 00/ 02978	26/10/2000	28/10/1999
Déposant		
BULL CP8		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé,**

   [X] le texte est approuvé tel qu'il a été remis par le déposant

   [ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° —

   [ ] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [X] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

[redacted] e Internationale No
PCT/FR 00/02978

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F7/72

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, PAJ, INSPEC, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 98 52319 A (YEDA RES & DEV ;FLEIT LOIS (US)) 19 novembre 1998 (1998-11-19) page 10, ligne 19 -page 12, ligne 5 ---	1
A	DIMITROV V ET AL: "TWO ALGORITHMS FOR MODULAR EXPONENTIATION USING NONSTANDARD ARITHMETICS" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES,JP,INSTITUTE OF ELECTRONICS INFORMATION AND COMM. ENG. TOKYO, vol. E78-A, no. 1, 1 janvier 1995 (1995-01-01), pages 82-87, XP000495124 ISSN: 0916-8508 * paragraphe 2.2 * --- -/--	1,3

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
19 janvier 2001	26/01/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Verhoof, P

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	BRICKELL E F ET AL: "FAST EXPONENTIATION WITH PRECOMPUTATION (EXTENDED ABSTRACT)" ADVANCES IN CRYPTOLOGY- EUROCRYPT. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES,DE,SPRINGER VERLAG, 24 mai 1992 (1992-05-24), pages 200-207, XP000577415 * paragraphe 2 *	1,3
A	KOCHER P C: "TIMING ATTACKS ON IMPLEMENTATIONS OF DIFFIE-HELLMAN, RSA, DSS, AND OTHER SYSTEMS" PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO),DE,BERLIN, SPRINGER, vol. CONF. 16, 1996, pages 104-113, XP000626590 ISBN: 3-540-61512-1 * paragraphe 10 *	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 00/02978

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9852319 A	19-11-1998	US 5991415 A	23-11-1999
		AU 7568598 A	08-12-1998
		EP 0986873 A	22-03-2000

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
3 mai 2001 (03.05.2001)

PCT

(10) Numéro de publication internationale
WO 01/31436 A1

(51) Classification internationale des brevets[7]: G06F 7/72

(21) Numéro de la demande internationale:
PCT/FR00/02978

(22) Date de dépôt international:
26 octobre 2000 (26.10.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) Données relatives à la priorité:
99/13507 28 octobre 1999 (28.10.1999) FR

(71) Déposant *(pour tous les États désignés sauf US)*: **BULL CP8** [FR/FR]; 68, route de Versailles, Boîte postale 45, F-78430 Louveciennes (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)*: **GOUBIN, Louis** [FR/FR]; 3, rue Brown Séquard, F-75015 Paris (FR).

(74) Mandataire: **BULL S.A.**; Corlu, Bernard, PC58D20, 68, route de Versailles, F-78434 Louveciennes cedex (FR).

(81) États désignés *(national)*: JP, US.

(84) États désignés *(régional)*: brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée:
— *Avec rapport de recherche internationale.*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: SECURITY METHOD FOR A CRYPTOGRAPHIC ELECTRONIC ASSEMBLY BASED ON MODULAR EXPONENTIATION AGAINST ANALYTICAL ATTACKS

(54) Titre: PROCEDE DE SECURISATION D'UN ENSEMBLE ELECTRONIQUE DE CRYPTOGRAPHIE A BASE D'EXPONENTIATION MODULAIRE CONTRE LES ATTAQUES PAR ANALYSE PHYSIQUE

(57) **Abstract:** The invention concerns a security method for an electronic assembly implementing a cryptographic computation process using a modular exponentiation of a quantity (x), said modular exponentiation utilising a secret exponent (d). The invention is characterised in that it consists in breaking down said secret exponent into a plurality of k unpredictable values (d_1, d_2, ..., d_k) whereof the sum is equal to said secret exponent.

(57) **Abrégé:** L'invention concerne un procédé de sécurisation d'un ensemble électronique mettant en oeuvre un processus de calcul cryptographique faisant intervenir une exponentiation modulaire d'une grandeur (x), ladite exponentiation modulaire utilisant un exposant secret (d), caractérisé en ce que l'on décompose ledit exposant secret en une pluralité de k valeurs imprévisibles (d_1, d_2, ..., d_k) dont la somme est égale audit exposant secret.

WO 01/31436 A1

PROCEDE DE SECURISATION D'UN ENSEMBLE ELECTRONIQUE DE CRYPTOGRAPHIE A BASE D'EXPONENTIATION MODULAIRE CONTRE LES ATTAQUES PAR ANALYSE PHYSIQUE

La présente invention concerne un procédé de sécurisation d'un ensemble électronique mettant en œuvre un algorithme faisant intervenir une exponentiation modulaire, dans laquelle l'exposant est secret. Plus précisément, le procédé vise à réaliser une version d'un tel algorithme qui ne soit pas vulnérable face à un certain type d'attaques physiques – dites « analyse d'énergie électrique différentielle ou analyse d'énergie électrique différentielle de haut niveau » (*Differential Power Analysis* ou *High-Order Differential Power Analysis*, en langage anglo-saxon, en abrégé DPA ou HO-DPA) - qui cherchent à obtenir des informations sur la clé secrète à partir de l'étude de la consommation électrique de l'ensemble électronique au cours de l'exécution du calcul.

Les algorithmes cryptographiques considérés ici utilisent une clé secrète pour calculer une information de sortie en fonction d'une information d'entrée ; il peut s'agir d'une opération de chiffrement, de déchiffrement ou de signature ou de vérification de signature, ou d'authentification ou de non-répudiation ou d'échange de clé. Ils sont construits de manière à ce qu'un attaquant, connaissant les entrées et les sorties, ne puisse en pratique déduire aucune information sur la clé secrète elle-même.

On s'intéresse donc à une classe plus large que celle traditionnellement désignée par l'expression *algorithmes à clé secrète* ou *algorithmes symétriques*. En particulier, tout ce qui est décrit dans la présente demande de brevet s'applique également aux algorithmes dits *à clé publique* ou *algorithmes asymétriques*, qui comportent en fait deux clés : l'une publique, et l'autre, privée, non divulguée, cette dernière étant celle visée par les attaques décrites ci-dessous.

Les attaques de type Analyse de Puissance Electrique, développées par Paul Kocher et *Cryptographic Research* (Confer document *Introduction to Differential Power*

Analysis and related Attacks by Paul Kocher, Joshua Jaffe, and Benjamin Jun, Cryptography Research, 870 Market St., Suite 1008, San Francisco, CA 94102, édition du document HTML à l'adresse URL : http://www.cryptography.com/dpa/technical/index.html) partent de la constatation qu'en réalité l'attaquant peut acquérir des informations, autres que la simple donnée des entrées et des sorties, lors de l'exécution du calcul, comme par exemple la consommation électrique du microcontrôleur ou le rayonnement électromagnétique émis par le circuit.

L'analyse d'énergie électrique différentielle est une attaque permettant d'obtenir des informations sur la clé secrète contenue dans l'ensemble électronique, en effectuant une analyse statistique des enregistrements de consommation électrique effectués sur un grand nombre de calculs avec cette même clé.

Cette attaque ne nécessite aucune connaissance sur la consommation électrique individuelle de chaque instruction, ni sur la position dans le temps de chacune de ces instructions. Elle s'applique de la même manière si on suppose que l'attaquant connaît des sorties de l'algorithme et les courbes de consommation correspondantes. Elle repose uniquement sur l'hypothèse fondamentale selon laquelle :

Hypothèse fondamentale : Il existe une variable intermédiaire, apparaissant dans le cours du calcul de l'algorithme, telle que la connaissance de quelques bits de clé, en pratique moins de 32 bits, permet de décider si deux entrées, respectivement deux sorties, donnent ou non la même valeur pour cette variable.

Les attaques dites par analyse d'énergie électrique de haut niveau sont une généralisation de l'attaque DPA décrite précédemment. Elles peuvent utiliser plusieurs sources d'information différentes : outre la consommation, elles peuvent mettre en jeu les mesures de rayonnement électromagnétique, de température, etc. et mettre en œuvre des traitements statistiques plus sophistiqués que la simple notion de moyenne, des variables intermédiaires moins élémentaires qu'un simple bit ou un

simple octet. Néanmoins, elles reposent exactement sur la même hypothèse fondamentale que la DPA.

Le procédé, objet de la présente invention, a pour objet la suppression des risques d'attaques DPA ou HO-DPA d'ensembles ou systèmes électroniques de cryptographie à clé secrète ou privée, faisant intervenir une exponentiation modulaire, dans laquelle l'exposant est secret.

Un autre objet de la présente invention est en conséquence une modification du processus de calcul cryptographique mis en œuvre par les systèmes électroniques de cryptographie protégés de manière que l'hypothèse fondamentale précitée ne soit plus vérifiée, à savoir qu'aucune variable intermédiaire ne dépend de la consommation d'un sous-ensemble aisément accessible de la clé secrète ou privée, les attaques de type DPA ou HO-DPA étant ainsi rendues inopérantes.

Premier exemple : l'algorithme RSA

Le RSA est le plus célèbre des algorithmes cryptographiques asymétriques. Il a été développé par Rivest, Shamir et Adleman en 1978. Pour une description plus détaillée de cet algorithme, on pourra utilement se reporter au document ci-après :

- R.L. Rivest, A. Shamir, L.M. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, 21, n°2, 1978, pp. 120-126,

ou aux documents suivants :

- ISO/IEC 9594-8/ITU-T X.509, *Information Technology - Open Systems Interconnection - The Directory: Authentication Framework*;
- ANSI X9.31-1, *American National Standard, Public-Key Cryptography Using Reversible Algorithms for the Financial Services Industry*, 1993;
- PKCS #1, *RSA Encryption Standard*, version 2, 1998, disponible à l'adresse suivante :

ftp://ftp.rsa.com/pub/pkcs/doc/pkcs-1v2.doc.

L'algorithme RSA utilise un nombre entier n qui est le produit de deux grands nombres premiers p et q, et un nombre entier e, premier avec $ppcm(p-1,q-1)$, et tel que $e \neq \pm 1 \bmod ppcm(p-1,q-1)$. Les entiers n et e constituent la clé publique. Le calcul en clé publique fait appel à la fonction g de Z/nZ dans Z/nZ définie par $g(x)=x^e \bmod n$. Le calcul en clé secrète fait appel à la fonction $g^{-1}(y)=y^d \bmod n$, où d est l'exposant secret (appelé aussi clé secrète, ou privée) défini par $ed \equiv 1 \bmod ppcm(p-1,q-1)$.

Les attaques de type DPA ou HO-DPA font peser une menace sur les mises en œuvre classiques de l'algorithme RSA. En effet , celles-ci utilisent très souvent le principe dit de *square and multiply* en langage anglo-saxon pour effectuer le calcul de $x^d \bmod n$.

Ce principe consiste à écrire la décomposition

$$d = b_{m-1}\cdot 2^{m-1} + b_{m-2}\cdot 2^{m-2} + \ldots + b_1\cdot 2^1 + b_0\cdot 2^0$$

de l'exposant secret d en base 2, puis d'effectuer le calcul de la manière suivante :

1. $z \leftarrow 1$;

pour i allant de $m-1$ jusqu'à 0 faire :

2. $z \leftarrow z^2 \bmod n$;
3. si $b_i = 1$ alors $z \leftarrow z \times x \bmod n$.

Dans ce calcul, on constate que parmi les valeurs successives prises par la variable z, les premières ne dépendent que de quelques bits de la clé secrète d. L'hypothèse fondamentale permettant l'attaque DPA est donc réalisée. On peut ainsi deviner par exemple les 10 bits de poids fort de d en s'intéressant aux mesures de consommation sur la partie de l'algorithme correspondant à i allant de $m-1$ à $m-10$. On peut ensuite continuer l'attaque en utilisant les mesures de consommation sur la partie de l'algorithme correspondant à i allant de $m-11$ à $m-20$, ce qui permet de trouver les 10

bits suivants de d, et ainsi de suite. On trouve finalement tous les bits de l'exposant secret d.

Une première méthode de sécurisation, et ses inconvénients

Une méthode classique (proposée par Ronald Rivest en 1995) pour protéger l'algorithme RSA contre les attaques de type DPA consiste à utiliser un principe de " blinding " (camouflage). On utilise le fait que :

$$x^d \bmod n = (x \times r^e)^d \times r^{-1} \bmod n$$

Ainsi le calcul de $y = x^d \bmod n$ se décompose en quatre étapes :

- On utilise un générateur aléatoire pour obtenir une valeur r ;
- On calcule : $u = x \times r^e \bmod n$;
- On calcule : $v = u^d \bmod n$;
- On calcule : $y = v \times r^{-1} \bmod n$.

L'inconvénient de cette méthode est qu'elle oblige, pour chaque calcul, à calculer l'inverse modulaire r^{-1} de la valeur aléatoire r, cette opération étant en général coûteuse en temps (la durée d'un tel calcul est du même ordre que celle d'une exponentiation modulaire telle que $u^d \bmod n$). Par conséquent, cette nouvelle implémentation (protégée contre les attaques DPA) du calcul de $x^d \bmod n$ est environ deux fois plus lente que l'implémentation initiale (non protégée contre les attaques DPA). En d'autres termes, cette protection du RSA contre les attaques DPA accroît le temps de calcul de **100%** environ (en supposant que l'exposant public e est très petit, par exemple $e=3$; si l'exposant e est plus grand, ce temps de calcul est encore plus grand).

Une deuxième méthode : le procédé de la présente invention

Selon l'invention, un procédé de sécurisation d'un ensemble électronique mettant en œuvre un processus de calcul cryptographique faisant intervenir une exponentiation modulaire d'une grandeur *(x)*, ladite exponentiation modulaire utilisant un exposant secret *(d)*, est caractérisé en ce que l'on décompose ledit exposant secret en une pluralité de *k* valeurs imprévisibles $(d_1, d_2, \ldots\ldots, d_k)$ dont la somme est égale audit exposant secret.

Avantageusement, lesdites valeurs $(d_1, d_2, \ldots\ldots, d_k)$ sont obtenues de la manière suivante :

a) *(k-1)* valeurs sont obtenues au moyen d'un générateur aléatoire ;

b) la dernière valeur est obtenue par différence entre l'exposant secret et les *(k-1)* valeurs.

Avantageusement, le calcul de l'exponentiation modulaire est effectué de la manière suivante :

a) pour chacune desdites *k* valeurs, on élève la grandeur *(x)* à un exposant comprenant ladite valeur pour obtenir un résultat, un ensemble de résultats étant ainsi obtenus ;

b) on calcule un produit des résultats obtenus à l'étape a).

Avantageusement, au moins l'une desdites *(k-1)* valeurs obtenues au moyen d'un générateur aléatoire a une longueur supérieure ou égale à 64 bits.

Des détails et avantages de la présente invention apparaîtront au cours de la description suivante de quelques modes d'exécution préférés mais non limitatifs, en regard de la figure unique annexée, représentant une carte à puce.

Selon l'invention, on utilise le fait que :

$si\ d = d_1 + d_2,\ alors\ x^d \bmod n = x^{d_1} \times x^{d_2} \bmod n$

Ainsi le calcul de $y = x^d \bmod n$ se décompose en cinq étapes :

- On utilise un générateur aléatoire pour obtenir une valeur d_1 ;
- On calcule : $d_2 = d - d_1$;
- On calcule : $u = x^{d_1} \bmod n$;
- On calcule : $v = x^{d_2} \bmod n$;
- On calcule : $y = u \times v \bmod n$.

L'avantage est que, de cette manière, il n'y a pas d'inverse modulaire à calculer. En général, le temps de calcul d'une exponentiation modulaire est proportionnel à la taille de l'exposant. Ainsi si on note α le rapport entre la taille de d_1 et la taille de d_2, on se rend compte que le temps total du calcul dans cette nouvelle implémentation (protégée contre les attaques DPA) est environ $(1+\alpha)$ fois le temps de calcul dans l'implémentation initiale (non protégée contre les attaques DPA).

Notons que, pour obtenir une valeur d_1 non prédictible, il est nécessaire que sa taille soit au moins de 64 bits.

Le procédé ainsi décrit rend inopérantes les attaques de type DPA ou HO-DPA décrites précédemment. En effet, pour décider si deux entrées (respectivement deux sorties) de l'algorithme donnent ou non la même valeur pour une variable intermédiaire apparaissant au cours du calcul, il ne suffit plus de connaître les bits de clé mis en jeu. Il faut également connaître la décomposition de la clé secrète d en k valeurs $d_1, d_2, \ldots, d_k$ telles que $d=d_1+d_2+\ldots+d_k$. Si on suppose que cette décomposition est secrète, et qu'au moins une des k valeurs a une taille d'au moins 64 bits, l'attaquant ne peut pas prévoir les valeurs de $d_1, \ldots, d_k$, et donc l'hypothèse fondamentale, qui permettait de mettre en œuvre une attaque de type DPA ou HO-DPA, n'est plus vérifiée.

Exemples :

1. Si n a une longueur de 512 bits, en choisissant de prendre une valeur aléatoire d_1 de 64 bits, on obtient $\alpha=1/8$, ce qui fait que cette protection du RSA contre les attaques DPA accroît le temps de calcul de **12.5 %** environ.
2. Si n a une longueur de 1024 bits, en choisissant de prendre une valeur aléatoire d_1 de 64 bits, on obtient $\alpha=1/16$, ce qui fait que cette protection du RSA contre les attaques DPA accroît le temps de calcul de **6.25%** environ.

Deuxième exemple : l'algorithme de Rabin

Nous considérons ici l'algorithme cryptographique asymétrique développé par Rabin en 1979. Pour une description plus détaillée de cet algorithme, on pourra utilement se reporter au document suivant :

- M.O. Rabin, *Digitized Signatures and Public-Key Functions as Intractable as Factorization*, Technical Report LCS/TR-212, M.I.T. Laboratory for Computer Science, 1979.

L'algorithme de Rabin utilise un nombre entier n qui est le produit de deux grands nombres premiers p et q, vérifiant en outre les deux conditions suivantes :

- p est congru à 3 modulo 8 ;
- q est congru à 7 modulo 8.

Le calcul en clé publique fait appel à la fonction g de Z/nZ dans Z/nZ définie par $g(x)=x^2 \bmod n$. Le calcul en clé secrète fait appel à la fonction $g^{-1}(y)=y^d \bmod n$, où d est l'exposant secret (appelé aussi clé secrète, ou privée) défini par $d=((p-1)(q-1)/4+1)/2$.

La fonction mise en jeu par le calcul en clé secrète étant exactement la même que celle utilisée par l'algorithme RSA, les mêmes attaques DPA ou HO-DPA sont applicables et font peser les mêmes menaces sur l'algorithme de Rabin.

Sécurisation de l'algorithme

Comme la fonction est exactement la même que celle du RSA, le procédé de sécurisation décrit dans le cadre du RSA s'applique de la même manière au cas de l'algorithme de Rabin. L'accroissement du temps de calcul provoqué par l'application de ce procédé est également le même que dans le cas de l'algorithme RSA.

L'invention peut être mise en oeuvre dans tout ensemble électronique effectuant un calcul cryptographique faisant intervenir une exponentiation modulaire, notamment une carte à puce 8 selon la figure unique. La puce inclut des moyens de traitement de l'information 9, reliés d'un côté à une mémoire non volatile 10 et à une mémoire volatile de travail RAM 11, et reliés d'un autre côté à des moyens 12 pour coopérer avec un dispositif de traitement de l'information. La mémoire non volatile 10 peut comprendre une partie non modifiable ROM et une partie modifiable EPROM, EEPROM, ou constituée de mémoire RAM du type "flash" ou FRAM (cette dernière étant une mémoire RAM ferromagnétique), c'est-à-dire présentant les caractéristiques d'une mémoire EEPROM avec en outre des temps d'accès identiques à ceux d'une RAM classique.

En tant que puce, on pourra notamment utiliser un microprocesseur autoprogrammable à mémoire non volatile, tel que décrit dans le brevet américain n° 4.382.279 au nom de la Demanderesse. Dans une variante, le microprocesseur de la puce est remplacé - ou tout du moins complété - par des circuits logiques implantés dans une puce à semi-conducteurs. En effet, de tels circuits sont aptes à effectuer des calculs, notamment d'authentification et de signature, grâce à de l'électronique câblée, et non microprogrammée. Ils peuvent notamment être de type ASIC (de l'anglais « Application Specific Integrated Circuit »). Avantageusement, la puce sera conçue sous forme monolithique.

Dans le cas de l'utilisation d'un tel ensemble électronique, l'invention consiste en un procédé de sécurisation d'un ensemble électronique comprenant des moyens de

traitement d'information et des moyens de mémorisation d'information, le procédé mettant en œuvre un processus de calcul cryptographique faisant intervenir une exponentiation modulaire d'une grandeur *(x)* stockée dans les moyens de mémorisation d'information, ladite exponentiation modulaire utilisant un exposant secret *(d)* stocké dans les moyens de mémorisation, caractérisé en ce que l'on décompose, grâce auxdits moyens de traitement d'information, ledit exposant secret lu dans lesdits moyens de mémorisation d'information en une pluralité de *k* valeurs imprévisibles $(d_1, d_2, \ldots\ldots, d_k)$ dont la somme est égale audit exposant secret, lesdites *k* valeurs imprévisibles étant stockées dans les moyens de mémorisation d'information.

Avantageusement, lesdites valeurs $(d_1, d_2, \ldots\ldots, d_k)$ sont obtenues de la manière suivante :

a) *(k-1)* valeurs sont obtenues au moyen d'un générateur aléatoire et stockées dans les moyens de mémorisation d'information ;

b) la dernière valeur est obtenue par différence entre l'exposant secret et les *(k-1)* valeurs, calculée grâce auxdits moyens de traitement d'information.

Avantageusement, le calcul de l'exponentiation modulaire est effectué de la manière suivante :

a) pour chacune desdites *k* valeurs, on élève la grandeur *(x)* à un exposant comprenant ladite valeur pour obtenir un résultat, un ensemble de résultats étant ainsi obtenus ;

b) on calcule un produit des résultats obtenus à l'étape a).

Avantageusement, au moins l'une desdites *(k-1)* valeurs obtenues au moyen d'un générateur aléatoire a une longueur supérieure ou égale à 64 bits.

REVENDICATIONS

1. Procédé de sécurisation d'un ensemble électronique mettant en œuvre un processus de calcul cryptographique faisant intervenir une exponentiation modulaire d'une grandeur *(x)*, ladite exponentiation modulaire utilisant un exposant secret *(d)*, caractérisé en ce que l'on décompose ledit exposant secret en une pluralité de *k* valeurs imprévisibles $(d_1, d_2, \ldots\ldots, d_k)$ dont la somme est égale audit exposant secret.

2. Procédé selon la revendication 1, caractérisé en ce que lesdites valeurs $(d_1, d_2, \ldots\ldots, d_k)$ sont obtenues de la manière suivante :

a) *(k-1)* valeurs sont obtenues au moyen d'un générateur aléatoire ;

b) la dernière valeur est obtenue par différence entre l'exposant secret et les *(k-1)* valeurs.

3. Procédé selon la revendication 1, caractérisé en ce que le calcul de l'exponentiation modulaire est effectué de la manière suivante :

a) pour chacune desdites *k* valeurs, on élève la grandeur *(x)* à un exposant comprenant ladite valeur pour obtenir un résultat, un ensemble de résultats étant ainsi obtenus ;

b) on calcule un produit des résultats obtenus à l'étape a).

4. Procédé selon la revendication 1, caractérisé en ce qu'au moins l'une desdites *(k-1)* valeurs obtenues au moyen d'un générateur aléatoire a une longueur supérieure ou égale à 64 bits.

5. Utilisation du procédé selon la revendication 1 dans une carte à puce comportant des moyens de traitement de l'information.

6. Utilisation du procédé selon la revendication 1 pour la sécurisation d'un processus de calcul cryptographique utilisant l'algorithme RSA.

7. Utilisation du procédé selon la revendication 1 pour la sécurisation d'un processus de calcul cryptographique utilisant l'algorithme de Rabin.

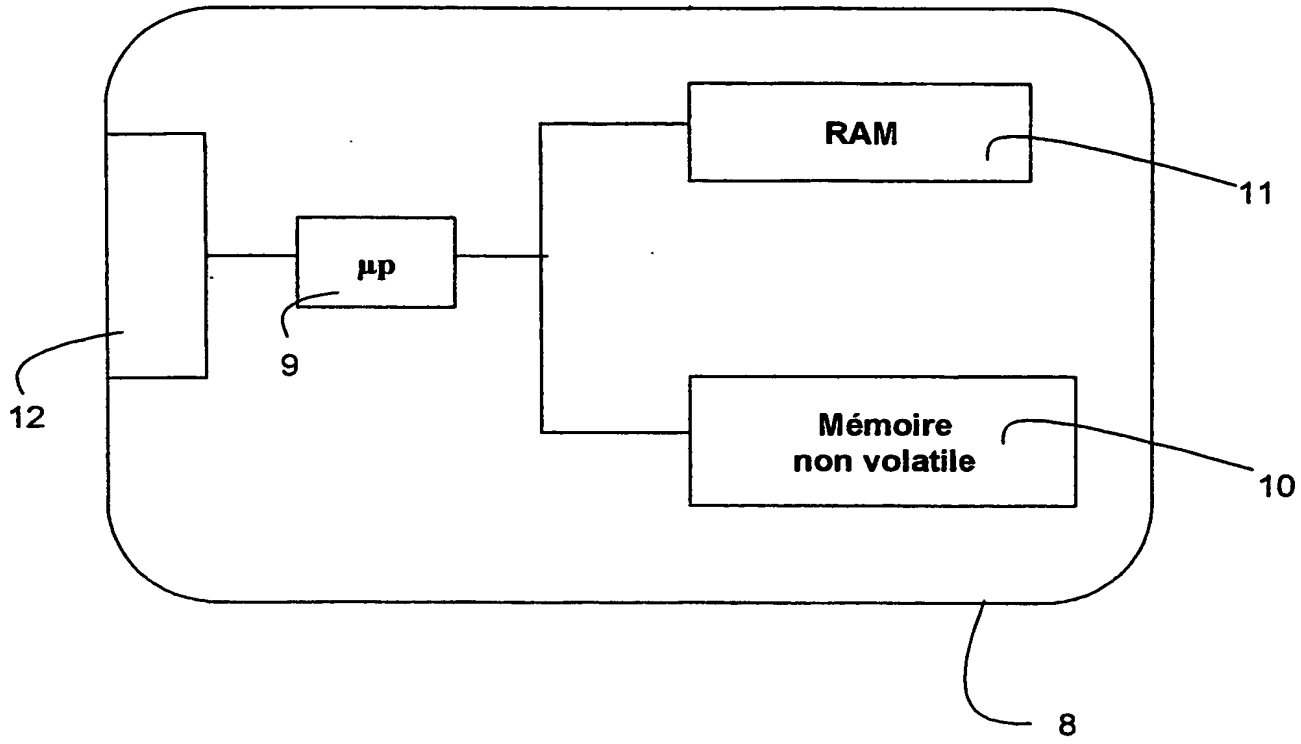

FIGURE UNIQUE